

SEALED

UNITED STATES DISTRICT COURT

for the
Western District of Virginia

DEC 11 2014

JULIA C. DUDLEY, CLERK
BY: *[Signature]*
DEPUTY CLERK

In the Matter of the Search of

*(Briefly describe the property to be searched
or identify the person by name and address)*In the Matter of the Search of Electronic Devices as
described in Attachment A, located at 116 North Main
Street Room 130, Harrisonburg, VA 22802

Case No. 5:14mj00078

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location)*:
Electronic Devices as described in Attachment A,located in the Western District of Virginia, there is now concealed *(identify the person or describe the property to be seized)*:The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☒ evidence of a crime;
- ☒ contraband, fruits of crime, or other items illegally possessed;
- ☒ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	Offense Description
18 U.S.C. Section 1029	Access Device Fraud
18 U.S.C. Section 1028A	Aggravated Identity Theft

The application is based on these facts:
See attached Affidavit

- ☐ Continued on the attached sheet.
- ☒ Delayed notice of 30 days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

[Signature]
Applicant's signatureL. McCAH BROTHERS SPA
Printed name and title

Sworn to before me and signed in my presence.

Date: 12-11-2014*[Signature]*
Judge's signatureCity and state: HARRISONBURG, VAJAMES G. WECSE, USMJ
Printed name and title

SEALED

IN THE UNITED STATES DISTRICT COURT FOR THE
WESTERN DISTRICT OF VIRGINIA
Harrisonburg Division

IN THE MATTER OF A SEARCH OF)
SAMSUNG GALAXY S4 SMARTPHONE)
BLACKBERRY BOLD SMARTPHONE)
DELL XPS DESKTOP COMPUTER/MONITOR)
SEAGATE 500GB SATA LAPTOP HARDDRIVE)
OPTICAL MEDIA QUANTITY 3 UNLABELED)
USB THUMB DRIVE 8 GB, BLACK/GRAY)
USB THUMB DRIVE, IMATION DEFENDER)
USB THUMB DRIVE, IMATION DEFENDER)
USB THUMB DRIVE, LABELED CAPITAL ONE)
USB THUMB DRIVE, LABELED LEXAR)
SEAGATE 320GB SATA LAPTOP HARDDRIVE)
USB THUMB DRIVE, IMATION DEFENDER)
USB THUMB DRIVE, LABELED IMATION)
ROCKETFISH EXTERNAL STORAGE DEVICE)
ASUS NEXUS TABLET, S/N: D60KBC021888)
SAMSUNG GALAXY SIII SMARTPHONE)
CURRENTLY LOCATED AT 116 NORTH MAIN)
STREET ROOM 130 HARRISONBURG, VA 22802)

Case Number: 5:14mj00078

AFFIDAVIT IN SUPPORT OF APPLICATION FOR A SEARCH WARRANT

I, Micah Bridges, Special Agent with the United States Department of State, Diplomatic Security Service ("DSS"), being duly sworn, state:

INTRODUCTION AND AGENT BACKGROUND

1. I have been employed as a Special Agent with the United States Department of State Diplomatic Security Service (DSS) since 2008. In that capacity I primarily investigate violations of federal statutes concerning identity theft, passport and visa fraud. I am presently assigned to the Washington Field Office as a criminal investigator specializing in cyber investigations and technical surveillance.
2. Prior to joining the DSS, I received my undergraduate education in accounting in 1999. I was employed as an officer with the Knox County Sheriff's Office, Knoxville, Tennessee

from 1999 to 2002. I was formally trained in 2008 as a Criminal Investigator at the Federal Law Enforcement Training Center in Glynco, Georgia and as a Special Agent at the DSS's Diplomatic Security Training Center in Dunn Loring, Virginia. My training included general law enforcement and criminal investigations, including identity theft, passport and visa fraud investigations. I have received specialized technical, cyber, and forensic training from the Federal Law Enforcement Center in Glynco, Georgia, and the Defense Cyber Investigations Training Academy, Baltimore, Maryland.

3. In my capacity as a Special Agent, I am currently conducting a joint investigation with Special Agent Chad Laub of the United States Secret Service into suspected violations of 18 U.S.C. §§ 1029 (Access Device Fraud) and 1028A (Aggravated Identity Theft).
4. This affidavit is submitted under Rule 41 of the Federal Rules of Criminal Procedure in support of an application for a warrant to search the following:
 - a. Samsung Galaxy S4 Smartphone, IMEI: 356567058635127
 - b. Blackberry Bold Smartphone, MEID: A00000262A1981, USDOC Label
#CD0002513792
 - c. Dell XPS Desktop computer/monitor combo, service Tag: 5Z5LDD1
 - d. Seagate 500GB SATA laptop harddrive S/N: 6VETJ5WD
 - e. Optical media quantity 3 unlabeled
 - f. USB Thumb Drive 8 GB, Black and gray in color
 - g. USB Thumb Drive, Imation Defender, 8GB, S/N: F21210460003013C
 - h. USB Thumb Drive, Imation Defender, 8GB, S/N: F212104600070147
 - i. USB Thumb Drive, labeled Capital One
 - j. USB Thumb drive, labeled Lexar

- k. Seagate 320GB SATA laptop harddrive, S/N: W0Q40B5H
 - l. USB Thumb Drive, Imation Defender, 8GB, S/N: F2121046000401F3
 - m. USB Thumb Drive, labeled Imation
 - n. Rocketfish external storage device
 - o. Asus Nexus Tablet, S/N: D60KBC021888
 - p. Samsung Galaxy SIII Smartphone, IMEI: 353091052421833
5. The items in paragraph 4 are collectively referred to as, the “Electronic Devices”, as more particularly described in Attachment A. The items have been in the custody of law enforcement since they were recovered from 7409 Lockport Place Suite D, Lorton, VA, the warehouse of AYALEX LLC AKA AYALEX GROUP, and 6909 Hamilton Court, Lorton, VA, the registered headquarters of AYALEX LLC and residence of Alexander Ayanou, the registered agent of AYALEX LLC, during the execution of federal search and seizure warrants at both locations on November 19, 2014, and they are currently at the United States Attorney’s Office for the Western District of Virginia located at 116 North Main Street, Room 130 Harrisonburg, Virginia 22802.
6. As explained in more detail below, I submit that there is probable cause to believe that the Electronic Devices contain evidence and constitute instrumentalities of conspiracy to commit access device fraud, in violation of 18 U.S.C. § 1029 and Aggravated Identity Theft in violation of 18 U.S.C. § 1028A.
7. The facts and information contained in this affidavit are based upon witness and suspect interviews and my review of records, documents, and other physical evidence obtained during this investigation, as well as information conveyed to me by other law enforcement officials. This affidavit does not include each and every fact known to the

government, but only those facts necessary to support a finding of probable cause to support the requested warrant.

BACKGROUND OF INVESTIGATION

8. In 2013, a joint investigation began between the Virginia State Police (“VSP”), the United States Department of State Diplomatic Security Service (“DSS”), and the United States Secret Service (“USSS”) into the unauthorized use of credit card account numbers to purchase and obtain numerous items from Home Depot and Lowe’s stores in Virginia and Maryland. Home Depot and Lowe’s are stores specializing in the sale of home furnishings, tools, and hardware.
9. Prior to the involvement of law enforcement, Home Depot and Lowe’s in the area began to notice an increase in the number of telephone and internet orders placed for merchandise resulting in an unusually large amount of “charge backs.” At Home Depot and Lowe’s stores there are service desks designed for construction and contracting professionals, large orders, pick up orders, telephone orders, and orders for customers with store accounts.
10. Based on my training and experience, I understand that, in this context, a “charge back” occurs when the credit card company notifies Home Depot and Lowe’s that the account holder has disputed the financial transactions allegedly made from their accounts by individuals using names different from the true account holders. The credit card companies notified Home Depot and Lowe’s that neither the credit card company nor the account holder was at fault for the disputed transactions, and, as a result, Home Depot and Lowe’s would most likely have to absorb the loss amount for the fraudulent

transaction. As a result, Home Depot and Lowe's began to scrutinize telephone and internet orders placed for pick up at the service desk using specific cellphone numbers, addresses, and fake names associated with known and suspected fraudulent credit card orders.

11. In August of 2013, DSS and USSS agents were investigating fraudulent credit card transactions at Home Depot and Lowe's stores using fraudulent customer names that did not match the true credit card account holder's names. During that same month, a Citibank investigator advised the DSS and USSS agents that a credit card with numbers ending in 6018 was identified as having been used in the fraudulent transactions in Virginia at Home Depot and Lowe's stores. Upon receiving that information, Home Depot and Lowe's regional investigators were contacted to identify the fraudulent transactions involving credit card number ending in 6018.
12. The fraudulent transactions for credit card number ending in 6018 involved telephone orders for a customer named Bob Lewis or a Robert/Bob Lewis with contact phone number (202) 374-4836. They were then picked up later by a third party person. A data base search for phone number (202) 374-4836 revealed it is connected to an address at 5400 Frazier Terrace in Fort Washington/Temple Hills, MD.
13. In March of 2014, Home Depot regional investigators identified additional fraudulent charges in Maryland and Virginia with another credit card account number ending in 2095. The fraudulent transactions at Home Depot for credit card number ending in 2095 involved telephone orders for a customer named Francis Young with a contact phone number of (571) 471-8388. The orders were then picked up by a third party person.

14. Investigators and agents have identified numerous fraudulent transactions at Lowe's stores in both the Western and Eastern Districts of Virginia using an American Express credit card number ending in 2095; which involved both telephone and internet orders for a customer named Francis Young or Francis Young with a contact phone number of (571) 471-8388. Those orders were also picked up later by a third party person, and several of the orders were picked up by CC-1 (Co-Conspirator "CC"). Agents from VSP, DSS and USSS identified three other suspects picking up fraudulent "Francis" orders that were purchased with the unauthorized credit card number ending in 2095 by CC-2, CC-3, and an individual named Steven Maurice Pemberton.
15. In April of 2014, Montgomery County, MD police detectives obtained a state of Maryland subpoena for subscriber information and calling records for (571) 471-8388. The call logs showed the (571) 471-8388 phone number called and received calls from some of the victim Lowe's and Home Depot store locations; including Lowe's stores in Winchester, VA, and a Home Depot store in Gaithersburg, MD. The (571) 471-8388 phone number also called or received calls associated with CC-1, CC-2, CC-3, and Steven Maurice Pemberton.
16. The call log for (571) 471-8388 also shows calls between it and a phone number (301) 237-9978, associated with Renodo Taylor. The call log for (571) 471-8388 also shows calls between it and a landline phone number (301) 630-8040, also associated with Taylor. Per Verizon internet service, both phone numbers (301) 237-9978 and (301) 630-8040 are associated Taylor's residence at 5400 Frazier Terrace, Temple Hills, MD.
17. In April of 2014, VSP agents obtained a state of Virginia Pen Order for (571) 471-8388. The Pen Order only collected a few phone numbers before the phone number became

inactive. The Pen Order recorded data that on April 16, 2014 that (703) 520-4471 called (571) 471-8388. Both phone numbers are associated with fraudulent credit card orders at Lowe's stores.

18. In June of 2014, VSP agents obtained a state of Virginia search warrant for Internet Protocol ("IP") addresses involved in numerous fraudulent credit card orders with card numbers ending in 2095, 4214, and 1530 at Lowe's store in Virginia, including a Lowe's store in Winchester, VA. Per Verizon, the IP addresses return back to customer account number 0138345950017, which is registered to a Renodo Taylor with electronic-mail address of taylor.renodo@yahoo.com at 5400 Frazier Terrace, Temple Hills, MD.
19. The fraud loss believed to be associated with Taylor and his co-conspirators from the unauthorized use of these credit card numbers at Home Depot and Lowe's stores is in excess of \$700,000.
20. Taylor also has a prior federal conviction from 2005 in the District of Columbia for access device fraud for using stolen credit card numbers to make unauthorized purchases. In that case he obtained more than 50 credit card numbers from a co-conspirator who worked in a grocery store. Taylor was then successful in making purchases with more than 30 of the card numbers. At the time, Taylor admitted to using the stolen card numbers to purchase flooring, refrigerators, washer/dryers, and other appliances that he would then resell for about 1/3 of the retail price.
21. In July 2014, a federal search warrant from District of Maryland, Greenbelt Division, was issued for Taylor's residence at 5400 Frazier Terrace, Temple Hills, MD. Agents from DSS and USSS served the search warrant at 5400 Frazier Terrace, Temple Hills, MD. During the search they seized computers, smart phones, and more than 200 credit card

numbers, including the credit card numbers ending in 6018 and 2095 that were known to the government to have been fraudulently used on numerous occasions. Most of the credit card numbers were on invoices from a high end catering service known to the government that is located in the Georgetown area of the District of Columbia. The catering invoices contained credit card numbers for numerous Chief Executive Officers and other Executives from prominent District of Columbia businesses, as well as Prominent Lobbying Firms, Large International Law Firms, and Multiple Congressional Offices - including the personal credit card number for a sitting United States Senator and one for the office of the then Majority Leader of the U.S. House of Representatives.

22. Agents contacted a supervisor from the catering company and were informed that Renodo Taylor was not authorized to have their invoices.

PROBABLE CAUSE

23. In August 2014, Renodo Taylor, with his attorney present, conducted a proffer session at the Western District of Virginia United States Attorney's Office, with your affiant, Special Agent Chad Laub, and the Assistant United States Attorney handling the investigation. During the proffer Taylor admitted to buying stolen credit card numbers from an associate he identified, and to purchasing numerous items with those numbers from several stores including Home Depot and Lowe's. Taylor also identified several subjects who transported and stored the fraudulently purchased merchandise for him. Taylor further stated that the subjects knew he was not a legitimate procurement source. Taylor stated sometimes he would call Pemberton to pick up the merchandise purchased with the stolen credit card numbers from the stores and then transport it to third parties.

Taylor also advised that Pemberton had previously stated that an associate from Africa was interested in purchasing merchandise from Taylor.

24. On or around September 5, 2014, a recorded telephone call was placed between Taylor and Pemberton with SA Bridges and SA Laub present. During this telephone conversation, Taylor told Pemberton that he was getting new card numbers and was going to order more merchandise. Taylor asked Pemberton if his African friend would be interested in purchasing the merchandise. Pemberton stated that the African will "take anything they can get their hands on," and would have the African call Taylor directly. On a later date the African called Taylor from cell phone number (571) 225-7486. A commercial database search indicated that the cell phone number (571) 225-7486 belongs to a Alexander Tete Ayanou. Further analysis showed that Alexander Ayanou owns and operates a company out of Lorton, Virginia, called AYALEX GROUP listed at 7409 Lockport Place D, Lorton, VA 22079. Corporate records also show another location for AYALEX as 6909 Hamilton Ct., Lorton VA 22079, with Alexander Ayanou as the Registered Agent at the same address.
25. On or around September 18, 2014, a recorded telephone call was placed between Taylor and Pemberton with SA Bridges and SA Laub present. During this conversation, Taylor told Pemberton he had an order at The Home Depot in Winchester, Virginia, that needed to be picked up. This was a controlled delivery order setup by Law Enforcement. Taylor told Pemberton that the order was under one of the fraudulent names he had previously used, Wilson Wilson, with a phone number of (301) 825-1372. Taylor told Pemberton that it needed to be delivered to Alexander Ayanou. The value of the items on the order was \$2,384.08. Pemberton picked up and delivered the merchandise to Ayanou as

requested. Ayanou said that he would pay Taylor \$500 for the whole lot. Taylor accepted the offer and the money was given to Pemberton for transporting the merchandise.

26. Also on or around September 18, 2014, Ayanou sent Taylor an email from "aayanou@gmail.com" to "hotrod14@mail.com" (the hotrod14@mail.com email was established and setup by SA Bridges specifically for this case). The email arrived from Ayanou with an attachment labeled as "gregg.xlsx". This spreadsheet listed 53 specific items Ayanou wanted Taylor to buy. The items listed in the spreadsheet consisted primarily of automotive repair equipment.

27. After identification of Alexander Ayanou and Ayalex Group as involved in the fraudulent activity, Chase Bank investigations was contacted to see if they had any known or suspected fraudulent activity involving Ayanou or Ayalex Group. Chase Investigations confirmed they had multiple transactions determined to be fraudulent involving Ayalex Group. Chase Bank Investigations fraudulent activity records show the following:

- a. Chase documentation reports that on March 25, 2014, a person using the name Tommy Rhodes contacted vendor Arctic Air Conditioning & Heating, Inc, 667 E. Ross Ave, El Centro, CA 92243 via email. Rhodes used the email address tommy_rhodes20@hotmail.com and placed an order for three (3) 1.5 Ton (18,000 BTU) Mitsubishi Straight-Cool Mini-Split Air Conditioning Systems, at a total cost of \$5,400.00. Initially Rhodes provided Visa Credit Card number 4147202137952642; however, it was declined. Notes from the vendor showed that they spoke to Tommy Rhodes on March 27, 2014, and he provided another MasterCard number 5418221611787257, with an address of 6406 Buckeye Path,

Grove City, OH 43123. That card was successfully charged the full amount. Tommy Rhodes also provided a prepaid FedEx Freight bill of lading 274796473-0, and the merchandise was delivered to Andrew Brown, Attention: Ayalex Group, 8050 Mims St. G, Lorton, VA 22079. Chase Bank Investigations later spoke with the actual cardholder, Jeri S. Stimson, and confirmed that the \$5,400 charge was fraudulent.

- b. On May 16, 2014, New Way Auto Parts, Inc., 1621 S. 4th Ave, Tucson, AZ 85713, received an order from a John Cole, 63 Barefoot Hill Rd, Sharon, MA 02067. Cole ordered a 2010 Mazda 3 Engine with a price of \$1,150. Cole provided credit card number 4388540031898116, and it was charged the full amount for the merchandise. Cole sent a prepaid FedEx Freight bill of lading 306469628-3 indicating that the engine was being shipped to Joe Brown, 5792 Dunster Ct #173, Alexandria, VA 22319. Cole also faxed a credit card authorization form to New Way Auto Parts, which included a signature and copies of the front/back of the credit card, and copy of the bio page of a United States Passport as identification. On May 27, 2014, FedEx Freight provided documentation showing the shipment number, 306469628-3, was reconsigned and delivered to Ayalex Group, 8050 Mims St G, Lorton, VA 22079. The reconsignment forms show that Andrew Brown was the person who authorized the reconsignment to Ayalex Group. Chase Bank Investigations confirmed with the actual cardholder that the charge was fraudulent.
- c. On May 19, 2014, Mas Auto Repair & SMOG Station, 980 S Claremont St, San Mateo, CA 94402 received an order from a Robert Smith for eight (8) Michelin

tires with a total value of \$2,718.14. Smith provided credit card number 5401683606349035, which was charged for the full amount. Smith also submitted a copy of the front/back of the credit card, and the bio page of a United States Passport as identification. Smith then sent a FedEx Freight prepaid bill of lading showing the merchandise to be delivered to Ayalex Group, 8050 Mims St G, Lorton, VA 22079. Chase Bank Investigations contacted the card holder and confirmed that the charge was fraudulent.

28. On or around November 13, 2014, a recorded telephone call was placed between Taylor and Alexander Ayanou with SA Laub present. During this conversation, Taylor told Ayanou that he received some new account numbers, but had some extra stuff that he needs to get rid of to make some money. Taylor told Ayanou that he had a dishwasher, Jenn-Air, and other tools, and asked if he was interested in buying the merchandise. Ayanou said that he was interested. Taylor said that he would have Pemberton bring it to him the next day. Taylor told Ayanou that he would use the money from that to pay for the new account numbers and start ordering the stuff off of Ayanou's list he sent during the week of September 15, 2014.

29. On or around November 13, 2014, a recorded telephone call was placed between Taylor and Pemberton with SA Laub present. Taylor told Pemberton he had an order at The Home Depot in Winchester, Virginia, that needed to be picked up. This was a controlled delivery order setup by Law Enforcement. Taylor told Pemberton that the order needed to be delivered to Alexander Ayanou. The value of the eight (8) merchandise items on the order was \$3,592.78. Taylor also told Pemberton that he was getting a bunch of new account numbers during the weekend, and would use the account numbers to order the

items off of the list that Ayanou sent him. Taylor told Pemberton that they would be busy with those new account numbers and would “have a good Christmas.” Pemberton picked up the order on November 14, 2014, from The Home Depot in Winchester, Virginia, and delivered the merchandise to Ayanou late on November 15, 2014. Taylor also received a call from Ayanou with the purpose of negotiating the price for the fraudulently purchased equipment. Taylor told SA Bridges that he told Ayanou he needed money so he could pay his contact for the new account numbers. Taylor told SA Bridges that Ayanou agreed to pay approximately \$500 for the items.

30. On or around November 19, 2014, law enforcement allowed a controlled purchase of a generator with a tracking device installed on it to occur. The purchase was made from a company called The Power Connection, Inc., a company located in Harrisonburg, Virginia. The generator was purchased using the fictitious name of John McHomer and using an address of 466 Main Street, Woodstock, VA 22664 on the invoice. The method of payment listed was an American Express card number ending with the last four digits of 2007.
31. As a part of the controlled purchase, law enforcement had Taylor contact Pemberton by telephone and advise him that he has just purchased two generators using new credit card numbers he has received. Pemberton agreed to transport one of the fraudulently purchased generators to Alexander Ayanou for him in return for his usual payment for doing so.
32. Taylor then called Alexander Ayanou and stated he just purchased two generators valued at over \$5,500, but the buyer backed out. Taylor asked Alexander Ayanou if wanted to buy them, and he agreed. Taylor also told Alexander Ayanou that after dropping off the

generator, Pemberton was going to Grainger Supply to pick up multiple items off the “gregg.xlsx” spreadsheet.

33. On or around November 19, 2014, the generators were delivered to Ayanou, and stored at an Ayalex Group facility located at 7409 Lockport Place D, Lorton, Virginia 22079.

NOVEMBER 19, 2014 SEARCH OF AYALEX LLC OFFICES

34. On November 19, 2014 federal search and seizure warrants were executed at 7409 Lockport Place Suite D, Lorton, VA, the warehouse of AYALEX LLC AKA AYALEX GROUP, and 6909 Hamilton Court, Lorton, VA, the registered headquarters of AYALEX LLC and residence of Alexander Ayanou, the registered agent of AYALEX LLC.
35. During the search, Alexander Ayanou was present at both locations and claimed to be the owner of AYALEX LLC.
36. During the execution of a federal search warrant of 7409 Lockport Place D, Lorton, VA, the eight (8) items from the controlled delivery set up by law enforcement from paragraph 29 were recovered. In addition, the generators from paragraphs 31-33 were recovered, as well as items addressed to Andrew Brown, Ayalex Group, the same name used in the fraudulent orders in paragraph 27a.
37. During the search, Alexander Ayanou was asked where all of the business documents and files for shipping were located. Ayanou stated that all of the documents were located at his residence, 6909 Hamilton Ct, Lorton, VA. This address was listed as the headquarters for Ayalex LLC. Directly after completing the search of 7409 Lockport Place D, Lorton,

VA, another federal search and seizure warrant was executed on 6909 Hamilton Ct, Lorton, VA.

38. During the execution of a federal search warrants at 7409 Lockport Place Suite D, Lorton, VA, the warehouse of AYALEX LLC AKA AYALEX GROUP, and 6909 Hamilton Court, Lorton, VA, the registered headquarters of AYALEX LLC and residence of Alexander Ayanou, the registered agent of AYALEX LLC, per the federal search warrant, the following Electronic Devices were seized during the search;

- a. Samsung Galaxy S4 Smartphone, IMEI: 356567058635127
- b. Blackberry Bold Smartphone, MEID: A00000262A1981, USDOC Label
#CD0002513792
- c. Dell XPS Desktop computer/monitor combo, service Tag: 5Z5LDD1
- d. Seagate 500GB SATA laptop harddrive S/N: 6VETJ5WD
- e. Optical media quantity 3 unlabeled
- f. USB Thumb Drive 8 GB, Black and gray in color
- g. USB Thumb Drive, Imation Defender, 8GB, S/N: F21210460003013C
- h. USB Thumb Drive, Imation Defender, 8GB, S/N: F212104600070147
- i. USB Thumb Drive, labeled Capital One
- j. USB Thumb drive, labeled Lexar
- k. Seagate 320GB SATA laptop harddrive, S/N: W0Q40B5H
- l. USB Thumb Drive, Imation Defender, 8GB, S/N: F2121046000401F3
- m. USB Thumb Drive, labeled Imation
- n. Rocketfish external storage device
- o. Asus Nexus Tablet, S/N: D60KBC021888

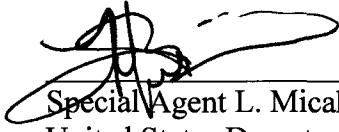
p. Samsung Galaxy SIII Smartphone, IMEI: 353091052421833

39. Based on my training and experience, I know that the smart phones have the capabilities that allow them to serve as wireless telephones, digital cameras, portable media players, global positioning system (or “GPS”) navigation devices, internet browsers, personal digital assistants, and as mass storage devices. In my training and experience, examining data stored on devices of this type can uncover, among other things, evidence that reveals or suggests who possessed or used the device.
40. Based on my training and experience, I know that electronic devices including smart phones, computer tablets, and computers can store information for long periods of time. Similarly, things that have been viewed via the Internet are typically stored for some period of time on the device. This information can sometimes be recovered with forensics tools.
41. As further described in Attachment B, this application seeks permission to locate not only electronically stored information that might serve as direct evidence of the crimes described on the warrant, but also forensic evidence that establishes how the Electronic Devices were used, the purpose of their use, who used them, and when. I submit that there is probable cause to believe that this forensic electronic evidence might be on Electronic Devices because:
- a. Data on a storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file).

- b. Forensic evidence on a device can also indicate who has used or controlled the device. This “user attribution” evidence is analogous to the search for “indicia of occupancy” while executing a search warrant at a residence.
- c. A person with appropriate familiarity with how an electronic device works may, after examining this forensic evidence in its proper context, be able to draw conclusions about how electronic devices were used, the purpose of their use, who used them, and when.
- d. The process of identifying the exact electronically stored information on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. Electronic evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, this application seeks authorization from the Court also to seize contextual information necessary to understand other evidence.

42. Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit the examination of the device consistent with the warrant. The examination may require authorities to employ techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of the device to human inspection in order to determine whether it is evidence described by the warrant.

43. Based on the foregoing, I submit that there is probable cause to believe that the Electronic Devices contain evidence of and constitute instrumentalities of conspiracy to commit access device fraud, in violation of 18 U.S.C. § 1029 and Aggravated Identity Theft in violation of 18 U.S.C. § 1028A.


Special Agent L. Micah Bridges
United States Department of State,
Diplomatic Security Service

Sworn to and subscribed before me
this 11th day of December, 2014.


United States Magistrate Judge

ATTACHMENT A

The property to be searched are the following devices (the "Electronic Devices"):

- Samsung Galaxy S4 Smartphone, IMEI: 356567058635127
- Blackberry Bold Smartphone, MEID: A00000262A1981, USDOC Label
#CD0002513792
- Dell XPS Desktop computer/monitor combo, service Tag: 5Z5LDD1
- Seagate 500GB SATA laptop harddrive S/N: 6VETJ5WD
- Optical media quantity 3 unlabeled
- USB Thumb Drive 8 GB, Black and gray in color
- USB Thumb Drive, Imation Defender, 8GB, S/N: F21210460003013C
- USB Thumb Drive, Imation Defender, 8GB, S/N: F212104600070147
- USB Thumb Drive, labeled Capital One
- USB Thumb drive, labeled Lexar
- Seagate 320GB SATA laptop harddrive, S/N: W0Q40B5H
- USB Thumb Drive, Imation Defender, 8GB, S/N: F2121046000401F3
- USB Thumb Drive, labeled Imation
- Rocketfish external storage device
- Asus Nexus Tablet, S/N: D60KBC021888
- Samsung Galaxy SIII Smartphone, IMEI: 353091052421833

All of these devices currently are located 116 North Main Street, Room 130, Harrisonburg, VA 22802.

ATTACHMENT B

1. All records on the Electronic Devices described in Attachment A that relate to violations of 18 U.S.C. § 1029 and involve Renodo Taylor since January 2012, including:
 - a. Telephone contact lists and call logs;
 - b. All records containing or related to credit card numbers and information;
 - c. All records containing or related to the purchase or sale of any items from Home Depot, Lowes, or other home improvement, construction, auto parts, or farm supply stores;
 - d. All digital photographs or videos related to the purchase or sale of any items from Home Depot, Lowes, or other home improvement, construction, auto parts, or farm supply stores
 - e. All digital documents related to the production or use of identity documents
 - f. All records related to the rental or use of trucks or shipping companies;
 - g. All records to, from, or regarding Renodo Taylor, Steve Pemberton , and other individuals involved in the access-device fraud conspiracy; and
 - h. All financial records.
2. Evidence of user attribution showing who used or owned the Electronic Devices and Computers at the time the things described in this warrant were created, edited, or deleted, such as logs, phonebooks, saved usernames and passwords, documents, and browsing history.

As used above, the terms “records” and “information” include all of the foregoing items of evidence in whatever form and by whatever means they may have been created or stored, including any form of computer or electronic storage (such as flash memory or other media that can store data) and any photographic form.

3. Forensic Analysis search.
 - a. Information, correspondence, records, documents or other materials constituting evidence of or pertaining to items “1a” through “1h” above, including:
 - i. Correspondence or communications, such as electronic mail, chat logs, and electronic messages;
 - ii. Internet usage records, user names, logins, passwords, e-mail addresses and identities assumed for the purposes of communication on the Internet, billing, account, and subscriber records, chat room logs, chat records, membership in online groups, clubs or services, connections to online or remote computer storage, and electronic files;
 - iii. Diaries, address books, names, and lists of names and addresses of individuals who may have been contacted by the computer and internet websites;
 - iv. Shared images, “friends lists” and “thumbnails”; and
 - v. Financial records, including credit card information.
 - b. The items listed in “a” through “g” above may be seized in whatever form, visual or aural, and by any means by which they may have been created, stored, or found, including:
 - i. Any computer, computer hardware (including input/output peripheral devices), computer software, router, computer-related documentation,

related peripherals, cellular phones, personal digital assistants, and digital cameras, including:

- * tapes, tape systems, and tape drives, cassettes, cartridges, streaming tapes, disks, disk drives, disk application programs, data disks, system disk operating systems, magnetic media floppy disks;
 - * hard drive and other computer related operation equipment;
 - * monitors, printers, modems, scanners;
 - * hardware and software manuals, passwords, data security devices;
 - * related documentation;
- ii. Handmade form, including writings, drawings, paintings;
- iii. Graphic Interchange formats and/or photographs, undeveloped photographic film, slides, and other visual depictions of such Graphic Interchange formats (including but not limited to JPG, GIF, TIF, AVI, MPG, and MPEG);
- iv. Mechanical form, including books, magazines, printing and typing;
- v. Electrical, electronic or magnetic form, including
- * tape recordings, cassettes, compact disks, backup tapes;
 - * electronic or magnetic storage devices such as floppy diskettes, hard disks, CD-ROMS, digital video disks (DVDs), Personal Digital Assistants (PDAs), Multimedia Cards (MMCs), memory sticks, flash memory devices, optical disks, printer buffers, smart cards, memory calculators, electronic dialers, or electronic notebooks;

- * digital data files;
 - * printouts or readouts from any magnetic, electrical or electronic storage device; and
- vi. Originals, photocopies, other copies and negatives.
- c. Records (maintained in all forms, including but not limited to handwritten, typed, computer generated) as follows:
 - i. Any and all documents, applications, records, mail, address and/or telephone notebooks, correspondence, books, receipts, notes, ledgers, and other papers and objects, including any computerized or electronic records, constituting or relating to any passport, visa, birth certificate, social security card, driver's license, marriage license, credit card, access device, passport photograph or similar photography, government identification card, or any other document that alone or in combination with others, may be used for identification or evidence of identity, including any records, relating to said items;
 - ii. Any and all documents records and objects, including computerized and electronic records, that refer to appliances, equipment, household purchases, or other reports;
 - iii. Any and all documents records and objects, including computerized and electronic records, that refer to passport sized photos;
 - iv. Any and all documents records and objects, including computerized and electronic records, that refer to FedEx, UPS, US Mail, bills of lading, or any other shipping and/or delivery receipts or packages;

- v. Any and all documents records and objects, including computerized and electronic records, that refer to bank statements, and bank signature documents connected with opening a bank account;
- vi. Any and all documents records and objects, including computerized and electronic records, that refer to credit card statements, and credit card signature documents connected with opening a credit account;
- vii. Any and all documents records and objects, including computerized and electronic records, that refer to correspondence with Sebastian Gyamfi or other identities as identified;
- viii. Any and all documents records and objects, including any computerized or electronic records relating to the Department of Homeland Security or the Immigration and Naturalization Service or that have been received from, or sent to, said agencies;
- ix. Any and all documents, records and objects, including computerized and electronic records, that refer or relate in any way to fraudulent birth certificate, identification documents, and financial documents;
- x. Any and all documents, records and objects, including computerized and electronic records, evidencing or relating to travel, domestic or international;
- xi. Any and all documents, photographs, letters, correspondence and other objects, including computerized and electronic records, relating to, or evidence of true or false identity;
- xii. Any and all passports or documents, including computerized or electronic records, that refer or relate to the obtaining or using of any passport;

- xiii. Any and all records reflecting indicia of occupancy, residency and/or ownership of the premises, including but not limited to utility and telephone bills, lease, mortgage, deed, lien records; U.S. Mail, including Express Mail, and other types of courier services;
 - xiv. Cellular telephones, computers, computer hardware, software, related documentation, computer passwords and data security devices, external storage devices (including, but not limited to, jump drives, thumb drives, CDs, and DVDs, that may contain any of the items listed above.
- d. The following definitions apply to the terms as set out in this affidavit and attachment:
- i. Computer hardware: computer hardware consists of all equipment, which can receive, capture, collect, analyze, create, display, convert, store, conceal, or transmit electronic, magnetic, or similar computer impulses or data. Hardware includes any data-processing devices (including but not limited to central processing units; cellular telephones, smartphones, internal and peripheral storage devices such as fixed disks, external hard drives, floppy disk drives and diskettes, and other memory storage devices); peripheral input/output devices (including but not limited to keyboards, printer, video display monitors, and related communications devices such as cables and connections), as well as any devices mechanisms, or parts that can be used to restrict access to computer hardware (including but not limited to physical keys and locks).

- ii. Computer Software: Computer software is digital information, which can be interpreted by a computer and any of its related components to direct the way they work. Software is stored in electronic, magnetic, or other digital form. It commonly includes programs to run operating systems, applications, and utilities.
- iii. Documentation: Computer-related documentation consists of written, recorded, printed, or electronically stored material, which explains or illustrates how to configure or use computer hardware, software, or other related items.
- iv. Passwords and Data Security Devices: Computer passwords and other data security devices are designed to restrict access to or hide computer software, documentation or data. Data security devices may consist of hardware, software or other programming code. A password (a string of alpha-numeric characters) usually operates a sort of digital key to “unlock” particular data security devices. Data security hardware may include encryption devices, chips, and circuit boards. Data security software of digital code may include programming code that creates “test” keys or “hot” keys, which perform certain pre-set security functions when touched. Data security software or code may also encrypt, compress, hide, or “booby-trap” protected data to make it inaccessible or unusable, as well as reverse the process to restore it.
- e. The computers may be searched for the following items: any and all items listed in item 3a above.

- i. Any of the items described in item 3a above which are stored in the form of magnetic or electronic coding on computer media or on media capable of being read by a computer with the aid of computer-related equipment, including floppy diskettes, fixed hard disks, removable hard disk cartridges, CDs, DVDs, thumb drives, software or memory in any form. The search procedure for the electronic data contained in computer operating software or memory devices shall include the following techniques which shall be used to minimize the risk that those conducting the search will view information not within the scope of the warrant:
- ii. Surveying various file “directories” and the individual files they contain (analogous to looking at the outside of a file cabinet for marking it contains and opening a drawer believed to contain pertinent files);
- iii. “opening” or cursorily reading the first few “pages” of such files in order to determine their precise contents;
- iv. “scanning” storage areas to discover and possibly recover recently deleted files;
- v. “scanning” storage areas for deliberately hidden files; or
- vi. Performing keyword or other search and retrieval searches through all electronic storage areas to determine whether occurrences of language contained in such storage areas exist that are intimately related to the subject matter of the investigation

- f. If after performing these procedures, the directories, files or storage areas do not reveal evidence of violations stated in affidavit, the further search of that particular directory, file, or storage area, shall cease.